Adapt Institute

# China's Cyber Threat: Implications for NATO and Potential Remedies

Lucia Kobzová

Adapt Long Read

This publication is supported by NATO's Public Diplomacy Division

**Author**
Lucia Kobzová
MA student of Public Policy with a focus on Digitalization at Sciences Po in Paris, France
Adapt Institute Junior Research Fellow

**Editor**
Matúš Jevčák
Editor-in-Chief at Adapt Institute

Adapt Long Read - Analytical Paper

September 2023

# CHINA'S CYBER THREAT: IMPLICATIONS FOR NATO AND POTENTIAL REMEDIES

*Lucia Kobzová*

## SUMMARY AND RECOMMENDATIONS

- China has rapidly grown in cyber power in recent years, leading to a significant increase in hacking activities directed at its adversaries, with NATO countries as the primary targets. Beijing's pursuit of offensive cyber operations aims to gain a strategic advantage in both the military and economic spheres on the global stage while also ensuring the continued rule of the Chinese Communist Party and the nation's security. However, in the West, these efforts are viewed with greater scepticism, as Chinese cyber activities are seen as a major threat to national security.
- The key shift in China's cyber strategy occurred during the 1990s when cyberspace was officially recognised as a strategic military domain. This shift was accompanied by substantial investments in the cyber army, followed by allocations to quantum technologies, cybersecurity, and other technological sectors. Various ministries and state institutions, often aided by hacktivists from the general public, carry out extensive cyberattacks against Chinese adversaries. The primary focus of these cyber efforts is on cyber espionage rather than traditional destructive attacks.
- The primary victim of Chinese cyber operations is the United States of America, NATO's largest member state. Washington has identified Beijing as the most significant cyber espionage threat to the nation, with an estimated annual theft of intellectual property exceeding $300 billion. Despite diverse diplomatic efforts to ease escalating cyber tensions, both sides continue with mutual offensive cyber operations.
- Other NATO member states also face relentless attacks from Chinese hackers, with cyber espionage being the most common technique. The frequency of these attacks is on the rise, accompanied by an increase in sophistication. Diplomatic entities, foreign ministries, the private sector, and various organisations are the most common targets. Furthermore, extensive data collection on NATO citizens occurs through Chinese social media platforms and companies, further enhancing Beijing's intelligence-gathering capabilities against its adversaries.

- To address the Chinese cyber threat, NATO should adopt a comprehensive set of measures. While the Alliance lags in technological capabilities, three potential solutions can enhance NATO's ability to respond effectively to cyber operations originating from Beijing:
    1. NATO should take a leading role in advocating for a new international treaty based on the principles outlined in the Tallinn Manual. Such a treaty could establish norms and standards for behaviour in cyberspace, fostering international cooperation and reducing the potential for cyber conflict.
    2. Substantial investments in the technological sector are essential, with a particular focus on improving cybersecurity measures and expanding quantum capabilities. These investments can strengthen NATO's cyber defences and enhance resilience against sophisticated cyber threats.
    3. Given the scale of the Chinese cyber threat, NATO must develop a comprehensive cyber strategy tailored specifically to address the challenges posed by China. This strategy should encompass elements of deterrence, resilience, and cooperation to effectively protect NATO's digital infrastructure and broader interests in an increasingly digitalised world.

## INTRODUCTION

In recent years, China has significantly expanded its global political influence, yet its remarkable economic growth has been accompanied by a series of actions that contravene international norms, particularly in the realm of cyberspace. The world has been captivated by China's hacking endeavours, which span across numerous countries and have brought the actions of the Chinese Communist Party (CCP) under international scrutiny. China has meticulously cultivated a formidable cyberinfrastructure, not solely for safeguarding its national security but primarily to leverage cyber capabilities for political, military, and economic advantages over Western nations. As Chinese President and General Secretary of the CCP, Xi Jinping, asserted: "China must pursue its aspiration to become a cyber power by reinforcing security and defence capabilities in cyberspace, promoting social governance through information technology, and advancing China's international influence and the formulation of cyberspace regulations" (Sen 2019).

According to the People's Republic of China's (PRC) agenda, the central priorities of the government are security, development, and sovereignty. These priorities are rooted in a broader political objective: preserving and securing the continued dominance of the CCP. Consequently, all government initiatives are directed toward fulfilling these priorities to a significant degree. One notable challenge facing the state is China's status as one of the most targeted nations for Distributed Denial of Service (DDoS) attacks in recent years. Additionally, the political leadership has accused the United States of America of engaging in cyber espionage and cyberattacks, as exemplified by the recent incident involving the Wuhan seismic laboratory (CyberWire 2023). However, such allegations remain difficult to substantiate, further fueling Beijing's efforts to bolster the state's cyber and technological capabilities. The CCP believes that the most effective way to defend information systems is by conducting offensive operations (Raud 2016). This not only diminishes other states' capacity to launch cyberattacks against China but, more importantly, furnishes the CCP with invaluable insights into the military and economic affairs of its adversaries. Beijing regards all cyber operations as strategically pivotal activities, albeit these strategic endeavours are understandably viewed with unease by Western powers.

In recent times, China has emerged as a formidable cyber threat to the United States and its North Atlantic Treaty Organization (NATO) partners. The number of cyberattacks originating from Chinese IP addresses has risen steadily, with particular concern over the rapid improvement in the efficiency and sophistication of these operations. China's investments in technological innovation, especially in quantum technologies crucial for cybersecurity, have solidified its position as a global leader (ChinaPower n.d.; Corbett and Singer 2022). The combination of this vast cyber apparatus, a sizable cyber army, and cutting-edge technological innovation has become one of the foremost challenges confronting NATO. Consequently, China is now recognised as a major cyber threat to NATO member countries.

## THE EVOLUTION OF THE CHINESE CYBER APPARATUS

The roots of China's efforts to bolster its cyber military capabilities can be traced back to the 1990s when national strategic military guidelines first mentioned the importance of winning wars in the context of modern technologies (Jinghua 2019). In subsequent years, cyberspace emerged as a pivotal domain for military operations (Jinghua 2019). The cyber realm was recognised as a critical pillar for socio-economic development and national security (Lu and Yuxiao 2015). China

subsequently adopted a range of internal documents and laws that underscored the significance of expanding its cyber army. These include the Cyber Security Law, National Cyber Security Strategy, National Strategy for Quantum Technologies, Document 26, and the International Strategy on Cooperation in Cyberspace (Raud 2016). Its military strategic doctrine posits that "cyber warfare is low-cost and highly effective, making it more likely to occur than other types of warfare." This may reflect the CCP's stance on cyber operations (Sen 2019).

The Chinese cyber apparatus comprises diverse entities, spanning formal units, militias, recruited criminals, and civilian volunteers (Booz, Allen, and Hamilton 2022). These groups operate under the purview of various governmental bodies, including the United Front Work Department, Propaganda Ministry, People's

**KEY PRC ORGANIZATIONS WITH CYBER MISSIONS**

This table characterizes several key PRC organizations with cyber missions. Significant overlaps in missions and authorities, joint operations, shared operational resources, and the use of common contractors contribute to the challenge of attributing PRC-aligned threat activity to specific organizations with high confidence.

| ORGANIZATION(S) | MAJOR MISSION AREAS | ACTIONS IN CYBERSPACE |
|---|---|---|
| PEOPLE'S LIBERATION ARMY | ★ National security<br>★ Military intelligence<br>★ Disaster relief<br>★ Peacekeeping | ★ Warfare<br>★ Military espionage<br>★ Economic espionage |
| MINISTRY OF STATE SECURITY | ★ Political security<br>★ Civilian intelligence<br>★ Counterintelligence | ★ Political espionage<br>★ Economic espionage<br>★ Dissident surveillance and harassment |
| MINISTRY OF PUBLIC SECURITY | ★ Domestic security<br>★ Public security<br>★ Law enforcement | ★ Content monitoring enforcement<br>★ Shaping IT regulations to support CCP political needs |
| CYBERSPACE ADMINISTRATION OF CHINA | ★ Internet governance<br>★ Internet regulation | ★ Regulation of cross-border data transfer, to include censorship via the national internet boundary system |
| CENTRAL PROPAGANDA DEPARTMENT (CPD) AND THE UNITED FRONT WORK DEPARTMENT (UFWD) | ★ National messaging | ★ Social media influence operations |
| GOVERNMENT CONTRACTORS | ★ N/A | ★ Support for or execution of agencies' offensive activities<br>★ Self-enriching data theft and ransom-ware operations |

Table: (Booz, Allen, and Hamilton 2022, 11)

Liberation Army, Ministry of State Security, and others (Booz, Allen, and Hamilton 2022). These state-aligned entities carry out cyber operations aligned with Beijing's strategic objectives, with a primary focus on the United States and its partners, as well as other adversaries in the Indo-Pacific region (Booz, Allen, and Hamilton 2022). More specifically, their activities in cyberspace target critical sectors such as logistics, energy, academia, and media (Raud 2016). The

overarching goal of these cyber activities is to gain political, military, and economic advantages over Western powers.

In the realm of cybersecurity, Beijing's strategy differs from other major cyber actors like Russia and Iran. Instead of conducting disruptive attacks aimed at damaging the critical infrastructure, China primarily engages in cyber espionage. Over the years, Beijing has become notorious for its extensive industrial and military cyber espionage activities. However, it's worth noting that, on occasion, Chinese hackers are responsible for attacks aimed at disrupting critical infrastructure. At the same time, Washington is increasingly concerned about potential hacks targeting its pipelines and other vital sectors (Satter, Siddiqui, and Pearson 2023). The most challenging aspect of Chinese cyber operations is their growing sophistication, attributed to the vast cyber apparatus and substantial investments in the technological and cybersecurity sectors. This complexity presents a significant challenge for victims in terms of detection and attribution. NATO, as one of the most relevant military adversaries of Beijing, is thus a prominent target of extensive cyber espionage campaigns.

## SINO-US CYBER RELATIONS OVER THE YEARS

China has been notably active in the cyberspace of the United States, the most militarily developed member of NATO. These interactions date back to the early 2000s when U.S.-China relations differed markedly from their contemporary state (Booz, Allen, and Hamilton 2022). At that time, China was granted regular trade relations and welcomed into the World Trade Organization (WTO). The U.S. National Security Strategy regarded China as a "peaceful and prosperous" emerging nation (Booz, Allen, and Hamilton 2022). However, this stance began shifting under the policies of President Obama, who opted for a stronger military presence in the Indo-Pacific region and a reorientation of foreign policies towards China (Booz, Allen, and Hamilton 2022). These changes also signalled a shift in strategic cyber priorities.

Subsequently, relations between the two nations have been marked by numerous conflicts and confrontations, largely driven by China's pursuit of becoming a global hegemon. Chinese cyber activities have played a central role in the consistent deterioration of Sino-US relations. China has deployed extensive espionage tools against the USA, with FBI Director Christopher Wray stating that Chinese espionage poses the most significant threat to the U.S. (AFP 2023). This aligns with the official stance of Washington, which views Beijing and

its cyber espionage campaigns as one of the most active and persistent threat actors (AFP 2023; CISA 2021; CISA 2023). According to estimates from the American National Security Bureau, China annually steals $300 billion from the U.S. through cyber espionage, primarily targeting intellectual property in the private sector. This strategy has proven effective, as Chinese companies benefit from the stolen patents, resulting in profits that fuel the growth of the Chinese economy. This approach enhances Beijing's international economic standing and provides a strategic advantage over its rivals.

One of the earliest cyberattacks with significant consequences for the U.S. occurred in 2010 (Mills 2010). Google was the primary target of this operation, but at least 20 organisations were affected. Chinese-aligned cybercriminal groups are believed to be behind the attack. These persistent Chinese cyber efforts led to dialogues between the leaders of the two nations in an attempt to de-escalate the tense cyber situation. However, these dialogues lasted only a year due to Beijing's refusal to continue interstate meetings (David 2023). Despite an agreement between President Obama and President Xi Jinping aimed at preventing further espionage and the theft of intellectual property, in 2015, the U.S. government's computer systems fell victim to a cyberattack (David 2023). This breach exposed the data of 21.5 million individuals, including healthcare and financial information. Furthermore, in 2019, the U.S. imposed sanctions on telecommunications company Huawei following the discovery of malicious cyber activities (Štrba 2019). As a result, the government banned the use of Huawei products in the country's infrastructure and advised the private sector against using Huawei-related solutions (Štrba 2019). Additionally, in 2021, the U.S. experienced another significant wave of cyber operations, with Washington attributing the attacks to the Chinese Ministry of Defense. This campaign primarily targeted Microsoft servers and other firms and organisations holding valuable information and patents (Conger and Frenkel 2021).

One of the most recent and concerning Chinese cyber campaigns targeted the American island of Guam (Sanger 2023). Chinese hackers affiliated with Volt Typhoon, a group believed to have direct ties to Beijing, were responsible for this breach. This operation held several key implications. Firstly, Guam occupies a strategically vital position, hosting essential military bases and ports crucial for a robust American response in the event of escalating conflict in the South China Sea. Guam also serves as the closest U.S. territory to Taiwan. Although the question of Taiwan's potential invasion has lingered for many years, the conflict

in Ukraine reignited debates regarding Chinese intentions toward the island, which Beijing considers part of its territory. The targets of the cyberattacks included a military base and critical sectors such as transportation and telecommunications, all crucial for mobilising forces during a crisis. Notably, the manner in which the cyberattack was executed marked a departure from typical cyber espionage tactics. A report published by Australia, the U.S., the U.K., New Zealand, and Canada indicated that the Chinese malware was not exclusively intended for cyber espionage (Kobzová 2023). The same malicious code could potentially be used to disrupt communication infrastructure and various services in the future. A breakdown in effective communication could lead to chaos and delayed responses. To evade detection, hackers took great care and infected home routers and internet-connected devices to gain remote access to victims' servers. These infected devices could serve as entry points to critical infrastructure. As mentioned earlier, Chinese hackers tend to favour cyber espionage over destructive attacks, making the malware discovered in Guam raises many questions.

## NATO VS CHINESE ESPIONAGE

The ongoing issue of constant cyber espionage is not limited solely to the largest and most influential NATO member. Other states within the Alliance also grapple with similar challenges when it comes to addressing Beijing's activities. IT company CheckPoint discovered that cyber-attacks originating from Chinese IP addresses against NATO member countries surged by 116% in 2022 (Check Point Research Team, 2022). The Intelligence and Security Committee of the British Parliament recently released a report concerning the Chinese threat to national security (Intelligence and Security Committee of Parliament, 2023). The primary concern raised in this report is the extensive espionage conducted within the UK's borders. This espionage encompasses data theft, cyber espionage, attacks against private sector entities and even governmental institutions.

Moreover, Chinese hackers consistently engage in cyber operations targeting European diplomatic entities. In July 2023, new cyber operations were identified in NATO countries such as Slovakia, the Czech Republic, Hungary, and others (Sharwood 2023). Just a few months prior to this, the European Union Agency for Cybersecurity (ENISA) issued a warning about multiple active Chinese advanced persistent threat (APT) actors within the EU (ENISA & CERT-EU, 2023). The ENISA report exposes numerous instances of cyber espionage attacks on member states, including activities directed at German companies, Belgian ministries,

French organisations, EU institutions, and numerous others (ENISA & CERT-EU, 2023). All NATO member states are consistently confronted with offensive cyber activities perpetrated by cybercriminal groups affiliated with Beijing. The scale and sophistication of these operations represent and will continue to pose a significant threat to NATO alliance cybersecurity.

In addition to the espionage campaigns, another serious concern stems from Beijing's extensive data collection efforts involving citizens of NATO countries. This collection is primarily facilitated through the social network TikTok and technological companies such as Huawei (Kaska, Beckvard, and Minárik 2019). Chinese companies are legally obligated to share all user data with the government. The extent of data collected raises numerous questions, as it far exceeds what is reasonably necessary for improving services for customers (Kaska, Beckvard, and Minárik 2019). Despite the requirement for all firms to store data within the EU and the US, there remains uncertainty regarding whether some data is surreptitiously transmitted to China. Data is regarded as an exceedingly valuable commodity, with some asserting that data is the most valuable asset on Earth. China is acutely aware of this fact, which is why it seeks access to data concerning the NATO population. This adds an entirely new dimension to NATO's cyber threat from China.

## SOLUTIONS FOR MITIGATING THE CHINESE THREAT

While Chinese cyber capabilities present a significant concern for NATO, there are several initiatives and measures that could be implemented to mitigate this threat.

Firstly, NATO should take a leading role within the international community in advocating for the adoption of an international treaty on cyberspace, building upon the existing Tallinn Manual. Discussions regarding the necessity of regulating cyberspace have only recently entered the public discourse. The UN Group of Governmental experts has concluded that existing international norms, including the UN Charter, apply to cyberspace (Raud 2016). However, these norms are insufficient, given the substantial differences between the physical and cyber realms. While legal experts agree that certain norms, such as the Geneva Conventions, could be applied to cyberspace, this would typically require human casualties, which is not the case for the majority of cyber operations. NATO has already developed a comprehensive guideline for international rules in cyberspace known as the Tallinn Manual (CCDCOE, n.d.). The challenge is that

the Tallinn Manual is not legally binding even for member states, necessitating its transformation into a formal legal framework. As a leader in this area, NATO should strongly advocate for a new international treaty governing cyberspace. Such a treaty would enhance global security and enable NATO to defend against Chinese threats more effectively. The international covenant would offer two key benefits: **serving as a deterrent** against cybercriminal activities by establishing a framework for **punishing perpetrators**. Presently, many cyber acts that might appear as criminal offences lack legal definitions, resulting in no legal consequences for wrongdoers. The criminalisation of certain acts may not deter all potential offenders, but it can reduce the likelihood of criminal activities occurring. This same logic can apply to Chinese hacking activities targeting NATO, which may decrease due to the deterrent effect of the cyber convention.

Secondly, NATO should significantly increase its investments in technological capabilities, both offensive and defensive. Chinese investments in technology, cybersecurity, and especially quantum technologies greatly outpace those of NATO allies. However, some initiatives are already underway, such as the creation of the Defence Innovation Accelerator for the North Atlantic (DIANA), aimed at fostering innovation, development, research, and cooperation across various sectors (Robinson 2023). More substantial financial resources are particularly needed in the quantum technologies sector to prevent what researchers refer to as the "quantum apocalypse." This scenario entails the complete breakdown of conventional cybersecurity measures once quantum computers are used for cyber operations. It is crucial to establish quantum-resistant infrastructure before China develops fully functional quantum computers, as Beijing is currently ahead of NATO in the quantum race (Corbett and Singer 2022; ChinaPower n.d.). Even if NATO cannot catch up in quantum computer development, it must implement measures to ensure effective post-quantum cryptography and encryption. Only through increased investments in technology can NATO remain competitive and ensure that member states' cybersecurity can withstand any threats originating from Beijing.

Last but not least, the Alliance should adopt a new strategic document outlining a comprehensive set of steps and measures to address the Chinese cyber threat. If Beijing is recognised as a security menace, there must be a specific plan to address the issue. Various initiatives have been proposed to address this lack of a coherent strategy, including the recent proposal by British Prime Minister Rishi Sunak for a tech-NATO strategy to counter technological challenges from China

(Jarnecki and Husch 2022). The challenge lies in the fact that member states have varying approaches. For instance, the United States opposes the use of Huawei technologies and has banned the firm's equipment from its infrastructure, while Germany and the Netherlands have adopted a more moderate approach (Jarnecki and Husch 2022). It is, therefore, imperative to unify member states' attitudes and behaviours under a single umbrella of a common strategy.

All of these efforts should be accompanied by cooperation with friendly countries and international organisations. Only through collaboration can NATO effectively defend itself against emerging cyber threats.

## CONCLUSION

China has significantly expanded its technological capabilities in recent years, utilising them to bolster its domestic political objectives and enhance its standing on the global stage. Beijing has successfully cultivated a skilled cadre of hackers who engage in cyber operations to achieve critical national strategic goals. The primary focus of these activities is on NATO countries, which are growing increasingly alarmed by the escalating Chinese cyber threat. The prevalent form of attack involves cyber espionage, through which Beijing annually siphons off millions of dollars from its adversaries and gains access to classified military documents. Coupled with its extensive data collection efforts targeting citizens of NATO nations through social media and tech companies, the Chinese government possesses exceptionally valuable information resources. NATO currently lags behind in terms of cybersecurity and technological capabilities. The cyber sector demands more substantial investments, with the bulk of financial resources necessary in the quantum realm, which will play a pivotal role in future defence strategies. Concurrently, NATO must formulate a comprehensive strategy for mitigating Chinese cyber threats and advocate for the establishment of an international cyber treaty building upon the principles of the Tallinn Manual. Undoubtedly, China represents the most formidable threat to NATO. The question that remains is how NATO will respond and whether it can regain ground in the ongoing cyber race, which it appears to be losing at present.

## REFERENCES

AFP. 2023. “Spies, hackers, informants: How China snoops on the US.” Security Week, February 8. Accessed August 20, 2023. https://www.securityweek.com/spies-hackers-informants-how-china-snoops-on-the-us/.

Booz, Allen, and Hamilton. 2022. “Same Cloak, More Dagger: Decoding How the People's Republic of China Uses Cyberattacks.” Boozallen.com. Accessed August 20, 2023. https://www.boozallen.com/content/dam/home/pdf/natsec/china-cyber-report.pdf.

CCDCOE. n.d. “The Tallinn Manual.” Accessed August 20, 2023. https://ccdcoe.org/research/tallinn-manual/.

Check Point Research Team. 2022. “Cyber Attacks from Chinese IPs on NATO Countries Surge by 116%.” Check Point, March 21. Accessed August 20, 2023. https://blog.checkpoint.com/security/cyber-attacks-from-chinese-ips-on-nato-countries-surge-by-116/.

ChinaPower. n.d. “Is China a Leader in Quantum Technologies?” Accessed August 20, 2023. https://chinapower.csis.org/china-quantum-technology/.

CISA. 2021. *CISA INSIGHT, Chinese Cyber Threat Overview and Actions for Leaders*. Accessed August 20, 2023. https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Chinese_Cyber_Threat_Overview_for_Leaders-508C.pdf.

CISA. 2023. *China Cyber Threat Overview and Advisories*. Accessed August 20, 2023. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china.

Conger, Kate, and Frenkel Sheera. 2021. “Thousands of Microsoft Customers May Have Been Victims to Hack Tied to China.” *New York Times,* March 6. Accessed August 20, 2023. https://www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html.

Corbett, Thomas, and Singer, W., Peter. 2022. “China May Have Just Taken the Lead in the Quantum Computing Race.” Defence One, April 14. Accessed August 20, 2023. https://www.defenseone.com/ideas/2022/04/china-may-have-just-taken-lead-quantum-computing-race/365707/.

CyberWire. 2023. “China accuses the US of interfering with earthquake response, Russia accuses the UK of assembling a Ukrainian Nazi assassin unit. Bots as moderators. Russia fines online platforms.” Accessed August 20, 2023. https://thecyberwire.com/newsletters/disinformation-briefing/5/33.

David, Hirschelf, Julie. 2015. “Hacking of Government Computers Exposed 21.5 Million People.” *New York Times*, July 9. Accessed August 20, 2023. https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html.

ENISA, and CERT-EU. 2023. *JP-23-01- Sustained activity by specific threat actors*. February 15. Accessed August 20, 2023. https://cert.europa.eu/static/files/TLP-CLEAR-JointPublication-23-01.pdf.

Intelligence and Security Committee of Parliament. 2023. *China*. July 13. Accessed August 20, 2023. https://isc.independent.gov.uk/wp-content/uploads/2023/07/ISC-China.pdf.

Jarnecki, Joseph, and Husch, Pia. 2022. “UK Leader´s Tech-NATO Proposal Won´t Tackle Chinese Technology Threats.” RUSI, November 3. Accessed August 20, 2023. https://rusi.org/explore-our-research/publications/commentary/uk-leaders-tech-nato-proposal-wont-tackle-chinas-technology-threats.

Jinghua, Lyu. 2019. “What Are China's Cyber Capabilities and Intentions?” Carnegie Endowment for International Peace, April 1. Accessed August 20, 2023. https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.

Kaska, Kadri, Beckvard, Henrik, and Minárik Tomáš. 2019. “Huawei, 5G, and China as a Security Threat.” CCDCOE. Accessed August 20, 2023. https://www.ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf.

Kobzová, Lucia. 2023. “Because of its strategic location it faces cyber-attacks. Why is China attacking the US island Guam?” Adapt Institute, June 7. Accessed August 20, 2023. https://www.adaptinstitute.org/because-of-its-strategic-location-it-faces-cyber-attacks-why-is-china-attacking-the-us-island-guam/07/06/2023/.

Lu, Xu, and Yuxiao, Li. 2015. “China's Cyber Security Situation and the Potential for International Cooperation.” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, edited by Jon R. Lindsay (ed.) et al., 225-241.*

*New York:* Oxford University Press. Accessed August 20, 2023. https://academic.oup.com/book/25744/chapter-abstract/193294854.

Mills, Eleanor. 2010. "Behind the China attack on Google (FAQ)." CNET, January 13. Accessed August 20, 2023. https://www.cnet.com/news/privacy/behind-the-china-attacks-on-google-faq/.

Raud, Mikk. 2016. "China and Cyber: Attitudes, Strategies, Organisation." CCDCOE. Accessed August 20, 2023. https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf .

Robinson, Karina. 2023. "Quantum Matters: NATO´s Quantum Leap: Designing a Quantum Strategy". *The Quantum Insider*, June 16. Accessed August 20, 2023. https://thequantuminsider.com/2023/06/16/quantum-matters-natos-quantum-leap-designing-a-quantum-strategy/.

Sanger, David. 2023. "Chinese Malware Hits Systems in Guam. Is Taiwan the Real Target?" *New York Times*, May 24. Accessed August 20, 2023. https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html.

Sharwood, Simon. 2023. "Undiplomatic Chinese threat actors attack embassies and foreign affairs departments." *The Register*, July 4. Accessed August 20, 2023. https://www.theregister.com/2023/07/04/smugx_europe_china_attack_europe/.

Satter, Raphael, Siddiqui, Zeba, and Pearson, James. 2023. "U.S. warns China could hack infrastructure, including pipelines, rail systems." *Reuters*, May 26. Accessed August 20, 2023. https://www.reuters.com/world/china/china-rejects-claim-it-is-spying-western-critical-infrastructure-2023-05-25/.

Sen, Guatam. 2019. "China´s Cyber Security Strategy: Global Implications." *Scholar Warrior,* Spring 2019: 128-134. Accessed August 20, 2023. https://archive.claws.in/images/journals_doc/1091385483_GautamSen.pdf.

Štrba, Pavol. 2019. "Ukradli nám Číňania naše technológie? O čom je kauza Huawei." Aktuality.sk, May 16. Accessed August 20, 2023. https://www.aktuality.sk/clanok/692188/huawei-cina-dusevne-vlastnictvo-explainer-vysvetlenie/.

Adapt Institute

Na vŕšku 8
811 01 Bratislava
Slovak Republic

office@adaptinstitute.org
+421 908 327 491
www.adaptinstitute.org